# Changing the Safety and Mission Assurance (S&MA) Paradigm

**Roy W. Malone, Jr., Director**
**Safety & Mission Assurance, MSFC**

**Fayssal M. Safie, Ph. D.**
**NASA Safety Center Tech. Fellow**

**PM Challenge 2010**
**7th Annual NASA Project Management Challenge**
**February , 2010**

# Agenda

- **Background**
- **Creating the environment**
- **The S&MA Paradigm shift**
- **The impact – Early involvement in the design process**
- **The S&MA path to the future**

# Background

## The Challenger report

- **Following the Space Shuttle Challenger accident, the Rogers Commission reported:**
  - S&MA not included in technical issue discussions
  - Inadequate S&MA staffing at MSFC – "Reductions in the safety, reliability and quality assurance work force at Marshall and NASA Headquarters have seriously limited capability in those vital functions (safety program responsibility) to ensure proper communications"
  - "A properly staffed, supported, and robust safety organization might well have avoided these faults (addressing faults within the S&MA organization that contributed to the Challenger Accident)…."

# Background

## The Columbia Report

- **Following the Space Shuttle Columbia accident, the Columbia Accident Investigation Board (CAIB) reported:**
  - "Throughout its history, NASA has consistently struggled to achieve viable safety programs and adjust them to the constraints and vagaries of changing budgets"
  - "The Board believes that the safety organization, due to a lack of capability and resources independent of the Shuttle Program, was not an effective voice in discussing technical issues or mission operations pertaining to STS-107."

# Background

## The 2006 NASA Exploration Safety Study

- **The 2006 NASA Exploration Safety Study (NESS) Team found that NASA "Safety and Mission Assurance is ineffective in carrying out its assigned responsibilities as given in the Governance document in many, but not all, NASA Centers." They cited:**
  - Lack of leadership
  - Lack of clearly defined lines of authority for action
  - Lack of clearly defined levels of responsibility for SMA requirements
  - Lack of technical excellence of personnel in the safety disciplines
  - Lack of personnel with domain knowledge
- **All of the above have led to lack of peer level respect from programmatic and engineering personnel and has rendered SMA ineffective.**

# Background

The message from the past

- **Common themes of all three efforts:**
  - Inadequate resources
  - Lack of discipline expertise
  - Lack of respect by engineering peers
  - Lack of inclusion in technical decisions
  - Lack of independence

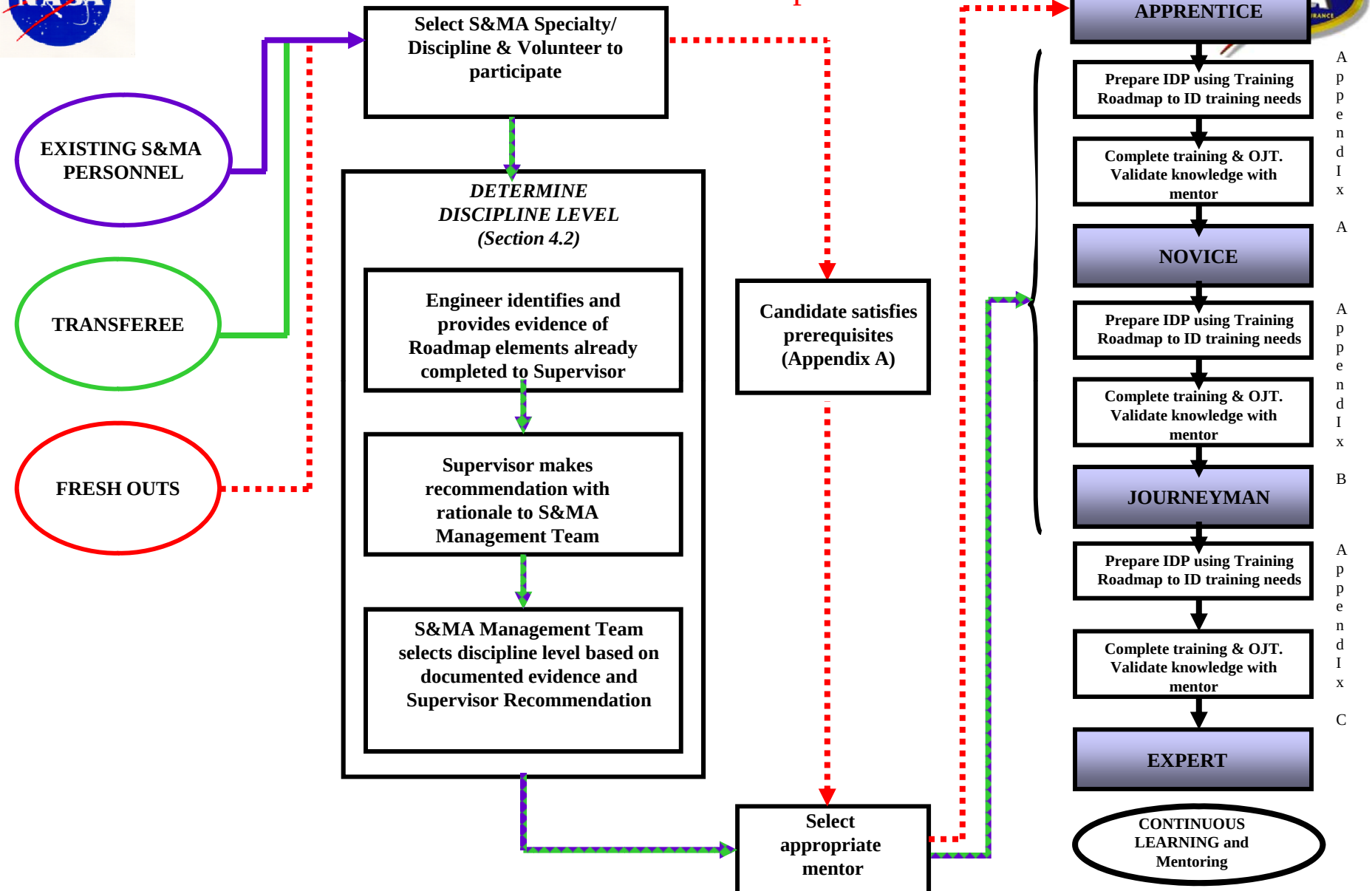
# Creating the Environment

## The Professional Development Roadmap

- **Overall Objective - Improve and maintain S&MA expertise and skills.**
- **Supporting Objectives:**
  - Develop a "Professional Development Roadmap" for each of the three main S&MA engineering disciplines (Systems Safety, R&M, and Quality Engineering).
    - Provide structured guidance for S&MA engineers to use in their efforts to become experts in their field.
      - Identify courses and knowledge that S&MA engineers need in order to develop their expertise.
      - Will base training on individuals current level of expertise.
    - Provide structured guidance to engineers in the development of their annual IDPs..

# Creating the Environment

## S&MA Professional Development Flow



# Creating the Environment

## The Professional Development Roadmap

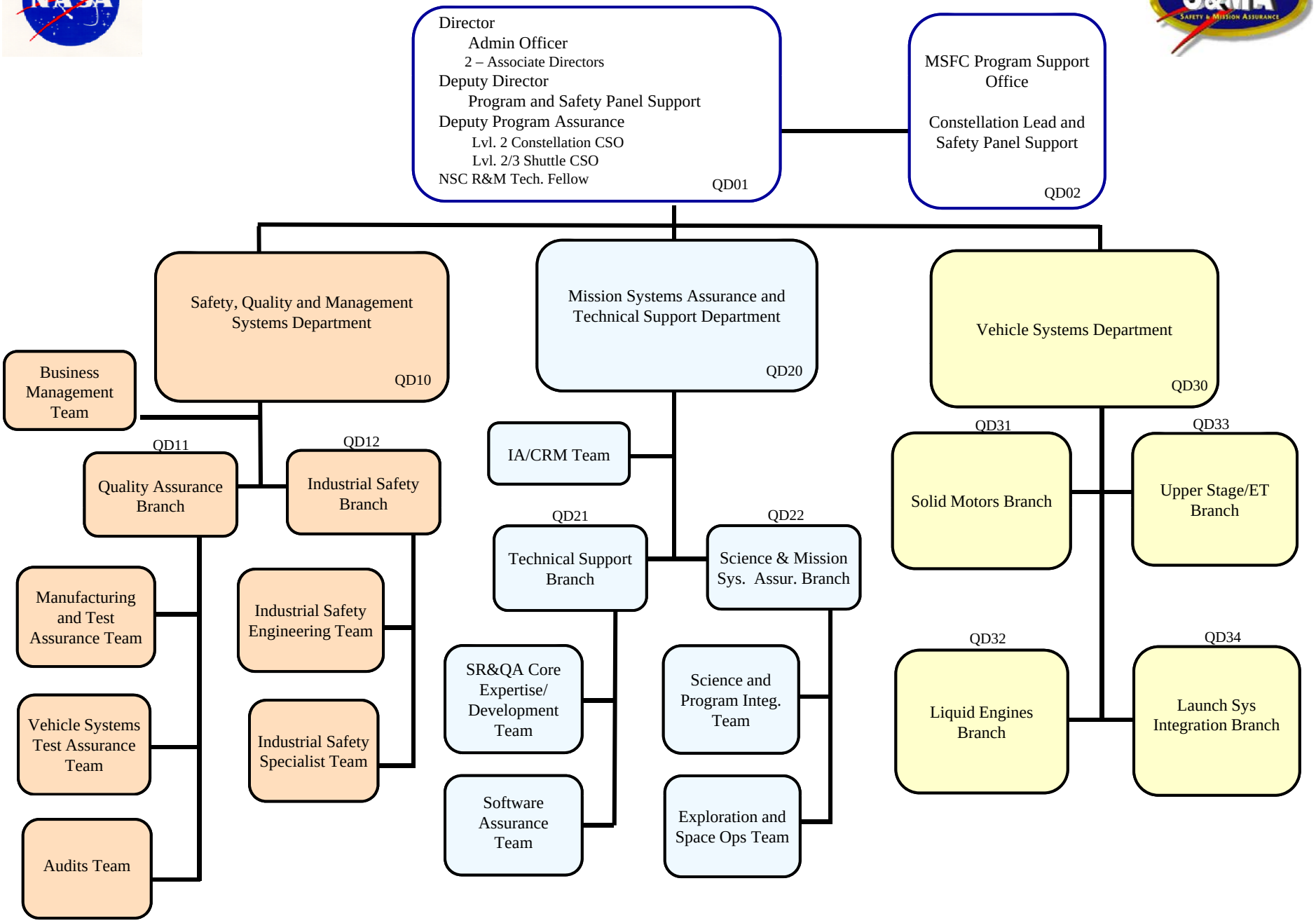
- **S&MA Discipline Training Roadmaps were expanded beyond Systems Safety, Reliability & Maintainability, and Quality Engineering to include:**
  - Auditor
  - Software Assurance
  - Industrial Safety Specialist
  - Quality Assurance

# Creating the Environment

## S&MA Re-organization

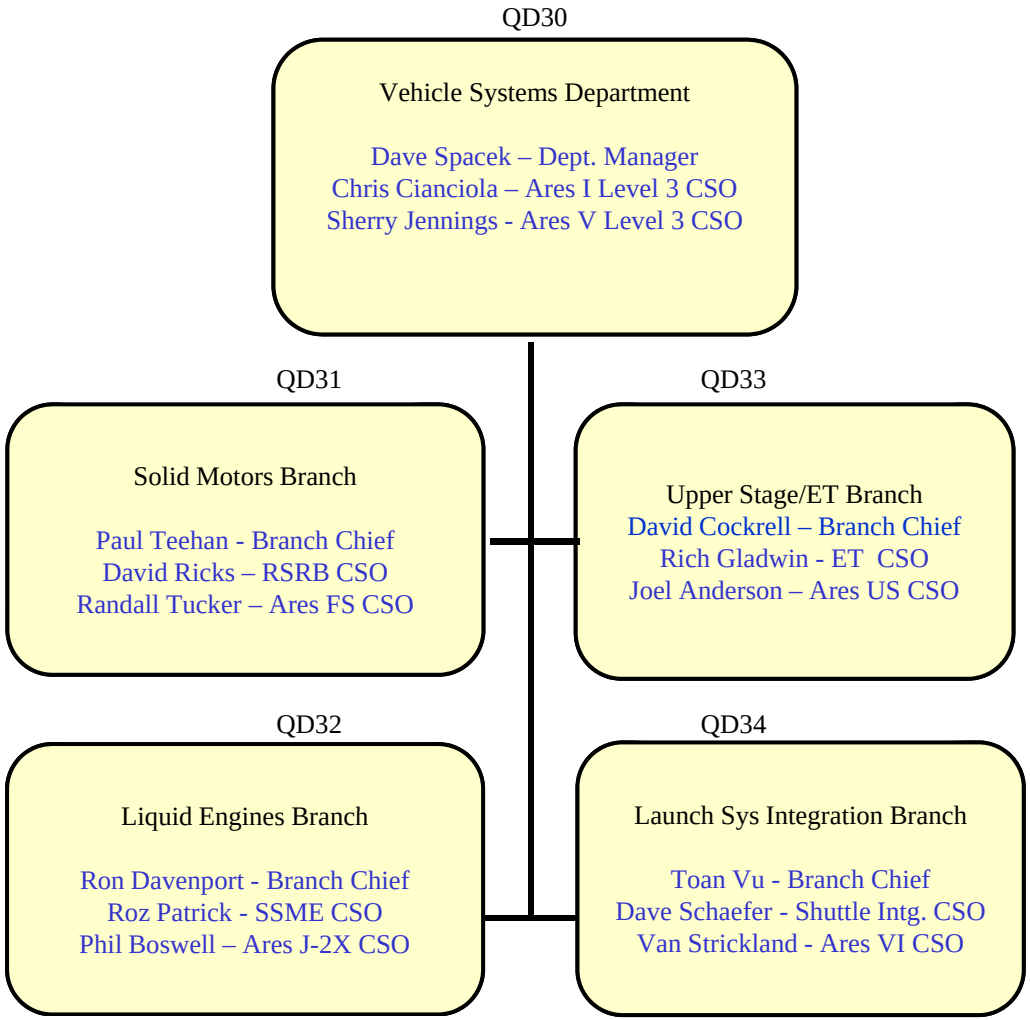
- **Objectives:**
  - Optimize S&MA organization to best facilitate Shuttle transition in 2010, successfully support Ares developmental responsibilities, and minimize the impacts of the gap between last shuttle flight and start of Ares V Project.
  - Improve leveraging of critical skills and experience between Shuttle and Ares.
  - Split technical and supervisory functions to facilitate technical penetration.
  - Create CSO (chief safety and mission assurance officer) stand-alone position for successfully implementation of S&MA Technical Authority.
  - Minimize disruption to customers.
  - Provide Early involvement of S&MA leadership team and frequent/open communications with S&MA team members and stakeholders.

# Creating the Environment - S&MA Re-organization



# Creating the Environment

## S&MA Re-organization



# Creating the Environment

## S&MA Re-organization

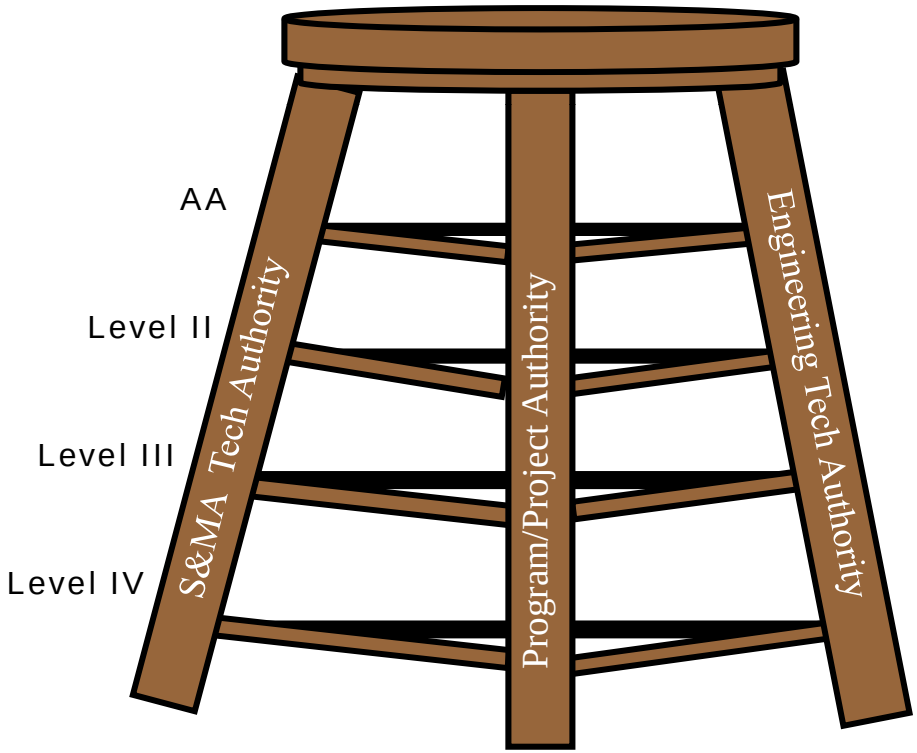
- **Chief Safety and Mission Assurance Officers (CSOs)**
  - Are equivalent to Element, Project and Program Chief Engineers.
  - CM&O TA funded.
  - Mainly responsible for project technical down and in.
  - Represent S&MA TA on assigned boards and panels.
  - Responsible for technical quality of organizational products.
- **Department Managers and Branch Chiefs**
  - Are the supervisors for the Level III and Level IV CSOs.
  - Can act for their CSOs and implement TA in their CSOs absence.
  - Are CM&O TA funded.
  - Responsible for the care, feeding and staffing of organization.
  - Represent S&MA TA on assigned boards and panels.
  - Responsible for the development of organizational technical products.

# Creating the Environment

## Post Columbia S&MA Enablers

- **Agency**
  - Created S&MA Technical Authority
  - Created NASA Safety Center
  - Created Discipline Fellows ST for S&MA Disciplines (in work)
- **MSFC**
  - Elevated MSFC S&MA Office to a Directorate
  - Elevated MSFC S&MA Deputy Director position to SES level
  - Created senior level engineering SES rotational position (every 2 years) in S&MA – Director for Program Assurance
  - Elevated Chief Safety and Mission Assurance Officer (CSO) positions to grade levels equivalent with MSFC Chief Engineers

# Technical Excellence



# The S&MA Paradigm shift

## The System Design Requirements Change

- **NASA has committed to a major space exploration program, called Constellation, intended to send crew and cargo to the International Space Station (ISS), to the moon, and beyond.**
- **In the past, space vehicle designers focused on performance.**
- **Lessons learned from the Space Shuttle and other launch vehicles show the need to optimize launch vehicles for other system parameters (reliability, safety, cost, availability, etc.) besides performance.**
- **The Constellation program has, therefore, put in place ambitious requirements for reliability, safety, and cost .**
- **The new requirements have forced a paradigm shift on how to design and build new launch vehicles which resulted in the creation of an integrated Risk-based design environment (e.g. Integrated analyses, disciplines, organizations, etc.) and the early involvement of S&MA in the design process**

# The S&MA Paradigm shift

## The S&MA Functional Roles Change

**Assurance:** Making certain that specified activities performed by others are performed in accordance with specified requirements. (Upper stage Engine and First Stage)

Examples of the activities include:

- Assess Hazard Analyses, FTAs, FMEA/CIL, PRA, etc.
- Approving Material Review Board (MRB) dispositions.
- Performing government inspections, audits, and surveillance.
- Independent assessments.
- Evaluating engineering and manufacturing changes, or proposed variances (adaptations, deviations, and waivers), for impacts to safety, reliability, and/or quality
- Evaluating the disposition of problems, including corrective actions (e.g., PRACA problem reports)

**In-Line** S&MA activities performed in direct support of the program/project to ensure that the program/project will achieve its objectives (Upper Stage and Vehicle Integration)

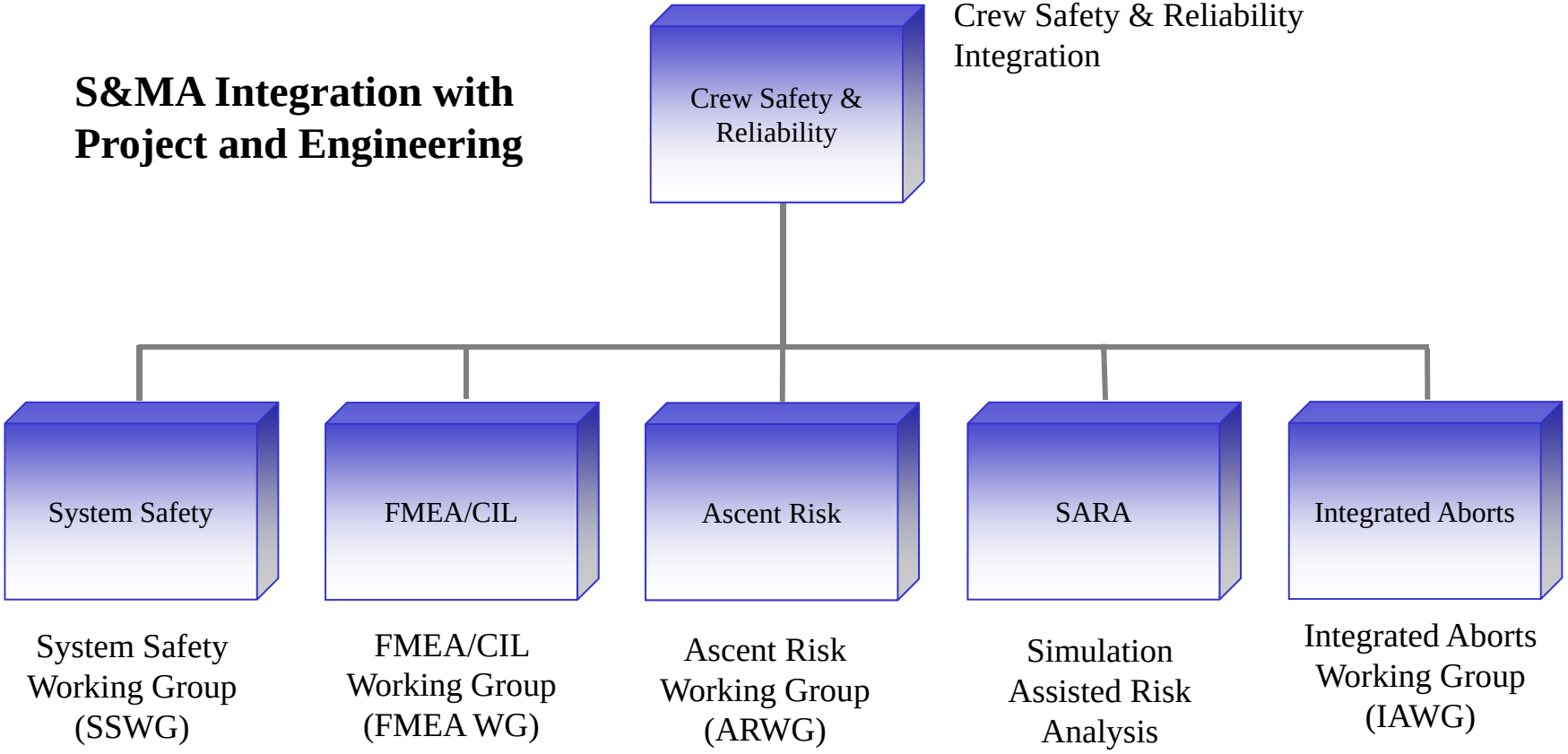
Examples of the activities include:

- Establish and implement S&MA programmatic and technical requirements.
- Perform Probabilistic Risk Assessments, Reliability Analysis, Integrated System Failure Analysis, Hazard Analyses, Fault Tree Analyses, FMEA/CIL, etc.
- Develop S&MA plans and methodologies.
- Establish and implement Industrial Safety.

# Creating the Environment

## The S&MA, project, and Engineering Integrated Operating Environment Change

**S&MA Integration with Project and Engineering**

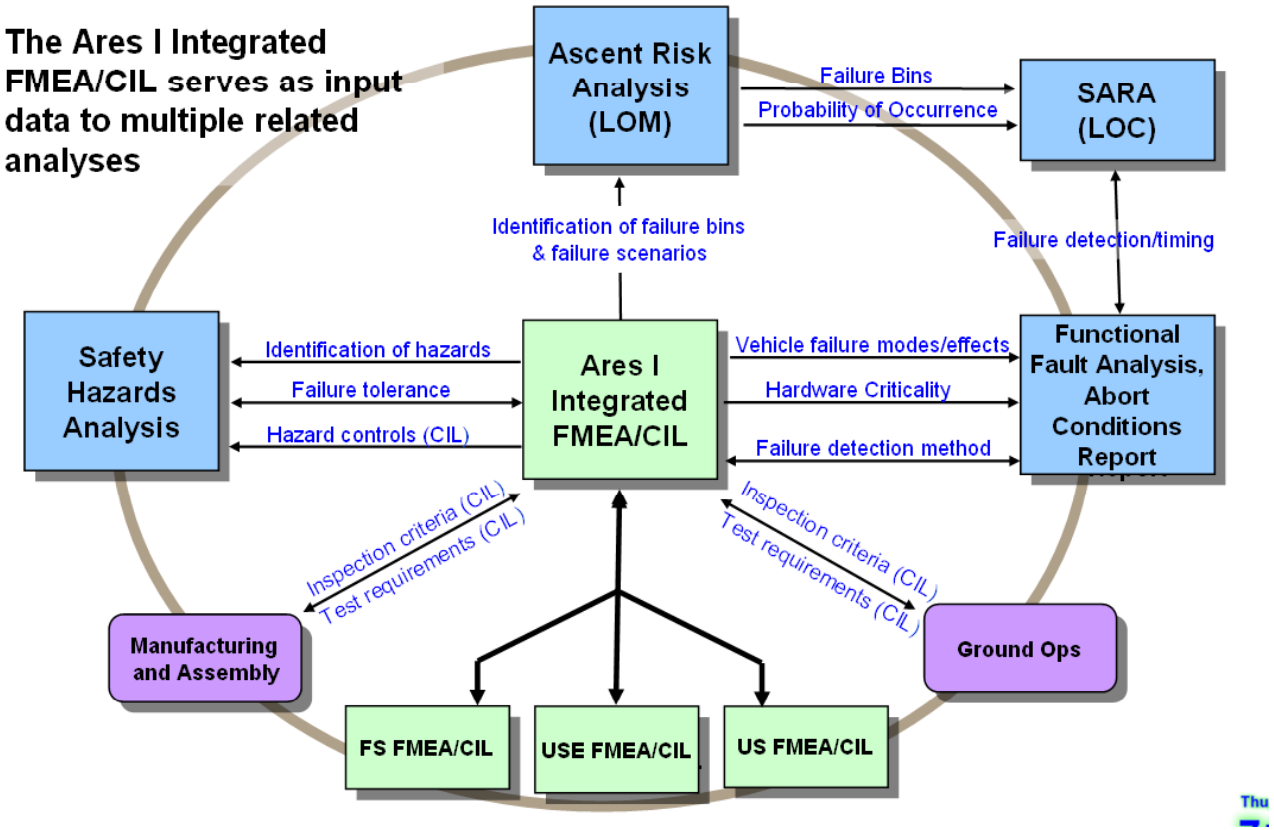


# Creating the Environment

The S&MA, project, and Engineering Integrated Operating Environment Change

## S&MA leading the Integrated FMEA Working Group

Integrated FMEA feeds other key analyses used to drive the safety and reliability of the Ares I design



# Creating the Environment

## The S&MA, project, and Engineering Integrated Operating Environment Change

- **S&MA leading the Ares I System Safety Working Group:**
  - Integrated Hazards
    - Identify hazard causes and controls that cross system and element boundaries and assure mitigation for the hazard causes
    - Ensure proper communication between Engineering (Design input for Hazard Controls) and S&MA – verify safety's understanding of vehicle design and ensure engineering design implementation of potential hazards
    - L2 – address hazards associated with Ares/Orion integrated stack → interface with Level 2 SE&I
    - L3 – address hazards associated with Ares vehicle → Ares VI S&MA
  - Assumed lead role in development of Fault Trees for Controls HR and Flight Termination System (FTS) HR to meet Phase 1 requirements (PDR)

# Creating the Environment

The S&MA, project, and Engineering Integrated Operating Environment Change

## S&MA leading the Ares I Ascent Risk Working Group

### Conceptual Design Phase

❑ **Support System Design**

- **Integrated system risk modeling and analysis**
- **System physics-based modeling and analysis**
- **Blast modeling for abort risk assessment**

### Design & Development Phase

❑ **Support Subsystem & Component Design**

- **Integrated with IPT's**
- **Component reliability modeling and analysis**
- **Integrated element modeling and analysis**
- **Component physics-based modeling and analysis**

### Operational Phase

❑ **Support System Risk Assessments**

- **Support launch issues**
- **Support upgrades**

# The impact – Early involvement in the design process

## Ares I Design impact (Examples)

- **Example of S&MA impact on the Ares I Design**
  - Influenced the choice of the solution to the Thrust Oscillation issue. Jointly working with engineering and Ares I project, S&MA assessed the reliability, quality and safety impacts of the various design solutions to the thrust oscillation issue. A lesson learned in "integrated failure analysis" from the Shuttle ET foam problem that contributed to the Columbia accident (Vehicle Integration)
  - Influenced the design solution to the First Stage-Upper Stage separation issue. Jointly working with engineering and Ares I project, S&MA assessed the reliability and safety impacts of the various design solutions to the First Stage-Upper Stage separation issue. Another lesson learned in "integrated failure analysis" from the Shuttle ET foam problem that contributed to the Columbia accident (Vehicle Integration)
  - Recommended pressurization line be moved out of cable tray to reduce risk to LSC and avionics (upper Stage)
  - Optimized valve design for reliability and safety for LH2 and LO2 pressurization.
  - Identified issue with use of KC fittings in safety-critical applications and approach to qualifying fittings as providing two seals (upper Stage)
  - Influenced the change of Linear Shape Charge (LSC) initiation timers from percussion to Flexible Confined Detonation Cord initiated timers (Flight Termination System)

# The impact – Early involvement in the design process

## Ares I Products (Examples)

- S&MA In-House Developed Products
  - Vehicle Integration - Crew Safety and Reliability Products
    - Ares I Failure Mode Effects Analysis/Critical Items List (FMEA/CIL)
    - Ares I System Safety Analysis Report (Hazard Analysis)
    - Ares I Fault Tree Analysis (FTA) Report
    - Ares I Ascent Risk Analysis (ARA) Report
    - Integrated Aborts Plan
    - Aborts Risk Assessment
  - Upper Stage S&MA Products
    - Safety, Reliability and Quality Plan
    - Failure Mode Effects Analysis
    - System Safety Analysis Report (including Fault Tree)
    - PRA Report
    - Reliability and Maintainability Analysis Report (Reference)
    - Limited Life Items List
- **Peer Review Products**
  - Upper Stage Engine and First Stage Peer Review
    - Quality Assurance Plan
    - System Safety Plan; Safety, Heath & Environment Plan
    - Reliability & Maintainability Program Plan
    - Failure Modes & Effects Analysis, Critical Items List, Limited Life Items
    - Reliability Allocations, Predictions & Analysis Report
    - Hazard Fault Tree Analysis Report

# The impact – Early involvement in the design process

## Are I Design Reviews (Example)

### Pre-Board Evaluation of PDR Success Criteria (7123.1A) (4 of 5)

| NPR 7123.1A Success Criteria. | Rating | Comments/Concerns |
|---|---|---|
| 7. Any required new technology has been developed to an adequate state of readiness, or backup options exist and are supported to make them a viable alternative. | G/Y | ♦ Gigabit Ethernet development is seen as poten[illegible] risk |
| 8. The project risks have been credibly assessed, and plans, a process, and resources exist to effectively manage them. | Y | ♦ Risk system to [illegible] programmatic ris[illegible]<br>♦ Coming out of P[illegible] identification and[illegible]<br>♦ Mitigation plans need t[illegible] red:<br>• Slosh Testing<br>• Development tes[illegible] educed in Upper Stage<br>— Resources were p[illegible] nsidered in scoring this criteria — |
| 9. Safety and mission assurance (e.g., safety, reliability, maintainability, quality, and EEE parts) have been adequately addressed in preliminary designs and any applicable S&MA products (e.g., PRA, system safety analysis, and failure modes and effects analysis) have been approved | G | ♦ **Excellent job of incorporating safety emphasis into the early requirements and design phase.** |

Of the 10 Ares PDR success criteria, S&MA was the only one rated entirely "Green" by the Pre-Board membership !

# The S&MA Path to the Future

- **We will continue building on our strength and the success path we started on Ares I.**
- **Ares I lessons learned are being used in supporting Ares V starting early in the conceptual design.**